PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-368870**
(43)Date of publication of application : **20.12.2002**

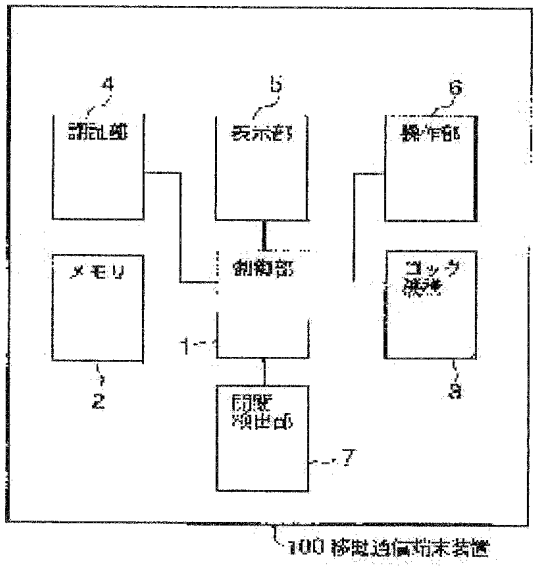
(51)Int.Cl. H04M 1/673
H04M 1/677
H04M 1/725

(21)Application number : **2001-167682**
(22)Date of filing : **04.06.2001**

(71)Applicant : **NEC CORP**
(72)Inventor : **MUTO TAKASHI**

(54) MOBILE COMMUNICATION TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a foldable mobile communication terminal that can limit use of other parties than a legitimate user.
SOLUTION: This invention provides the mobile communication terminal where 1st and 2nd cases are connected by an opening/closing means. The mobile communication terminal is provided with a lock means that locks a closing state of the opening/closing means, an opening/closing detection means that detects that the lock means locks the opening/closing means, an authentication means that authenticates pre-registered user, and a control means that releases locking by the lock means depending on the authentication result by the authentication means.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－368870
（P2002－368870A）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード(参考)
Ｈ０４Ｍ　1/673		Ｈ０４Ｍ	1/673	５Ｋ０２７
1/677			1/677	
1/725			1/725	

審査請求　未請求　請求項の数12　ＯＬ　（全　７　頁）

(21)出願番号　特願2001－167682(P2001－167682)

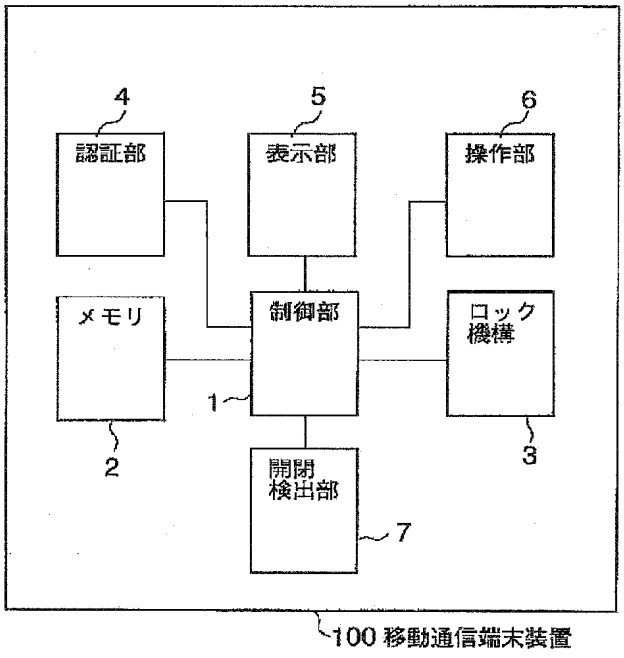
(22)出願日　平成13年６月４日(2001.6.4)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　武藤　貴志
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100071272
弁理士　後藤　洋介　（外１名）

Ｆターム(参考)　5K027 AA11 BB09 HH13 HH23

(54)【発明の名称】　移動通信端末装置

(57)【要約】
【課題】　正規の利用者以外の者による利用を制限することができる折り畳み型移動通信端末装置を提供すること。
【解決手段】　第１及び第２の筐体を開閉手段で接続した折り畳み型の移動通信端末装置。開閉手段が閉じた状態をロックするロック手段と、ロック手段が開閉手段をロックしていることを検知する開閉検出手段と、予め登録された利用者を認証する認証手段と、認証手段による認証結果に応じて、ロック手段によるロックを解除する制御手段とを備える。



1

【特許請求の範囲】

【請求項１】　第１及び第２の筐体部を開閉手段で接続した折り畳み型の移動通信端末装置において、
前記開閉手段が閉じた状態をロックするロック手段と、
前記ロック手段が前記開閉手段をロックしていることを検知する開閉検出手段と、
予め登録された利用者を認証する認証手段と、
前記認証手段による認証結果に応じて、前記ロック手段によるロックを解除する制御手段とを備えることを特徴とする移動通信端末装置。

【請求項２】　請求項１に記載の移動通信端末装置において、
前記第１及び第２の筐体のそれぞれが、接合部材により互いに嵌合する少なくとも２つの部材からなり、
前記接合部材の少なくとも一部は、前記開閉手段が閉じた状態にあるとき前記第１及び第２の筐体により隠蔽され、前記開閉手段が開いた状態にあるとき露呈することを特徴とする移動通信端末装置。

【請求項３】　請求項２に記載の移動通信端末装置において、前記接合部材はネジであり、隠蔽されるのは前記ネジの頭部であることを特徴とする移動通信端末装置。

【請求項４】　請求項１乃至３のいずれかに記載の移動通信端末装置において、取り外し可能な装置と接続するためのインタフェースを備え、前記開閉手段が閉じた状態で前記インタフェースを隠蔽することを特徴とする移動通信端末装置。

【請求項５】　請求項４に記載の移動通信端末装置において、前記取り外し可能な装置は記憶装置であることを特徴とする移動通信端末装置。

【請求項６】　請求項１乃至５のいずれかに記載の移動通信端末装置において、前記制御手段は、
前記開閉検出手段によって、前記開閉手段が閉じた状態にあることを検出した時間が予め定められた時間を経過すると、
前記ロック手段によって、前記開閉手段をロックすることを特徴とする移動通信端末装置。

【請求項７】　請求項１乃至６のいずれかに記載の移動通信端末装置において、
前記ロック手段が前記開閉手段をロックすると、受け付ける操作を制限し、
前記認証手段が前記利用者を認証すると、前記制限を解除することを特徴とする移動通信端末装置。

【請求項８】　請求項１乃至７のいずれかに記載の移動通信端末装置において、前記認証手段は、指紋に基づいて認証を行うことを特徴とする移動通信端末装置。

【請求項９】　請求項１乃至７のいずれかに記載の移動通信端末装置において、前記認証手段は、音声入力手段を含み、音声に基づいて認証を行うことを特徴とする移動通信端末装置。

【請求項１０】　請求項１乃至７のいずれかに記載の移動通信端末装置において、前記認証手段は、押下するキーの組み合わせに基づいて認証を行うことを特徴とする移動通信端末装置。

2

【請求項１１】　請求項１乃至７のいずれかに記載の移動通信端末装置において、前記認証手段は、画像入力手段を含み、入力された画像に基づいて認証を行うことを特徴とする移動通信端末装置。

【請求項１２】　請求項１乃至７のいずれかに記載の移動通信端末装置において、前記認証手段は、無線受信手段を含み、外部装置から無線を介して入力された情報に基づいて認証を行うことを特徴とする移動通信端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯電話やＰＨＳ（Personal Handy Phone System）等の移動通信端末装置に関する。特に、本発明は、移動通信端末装置に格納されている情報の漏洩を防ぐ技術に関する。

【０００２】

【従来の技術】一般に、最近の移動通信端末装置は、電子メールの送受信、アドレス帳、メモ等の様々な機能を備えることが多く、その結果、メールアドレス、電話番号、住所といった個人情報を大量に格納することになる。大半の移動通信端末装置では、操作方法さえ知っていれば誰でも格納しているデータを参照できるようになっている。このため、移動通信端末装置を置き忘れてしまったり、盗難に遭ってしまった場合、持ち主の個人情報が第三者に漏洩してしまう可能性が非常に高いという問題がある。

【０００３】この問題を解決するため、従来の移動通信端末装置には、所定の操作により主要な機能をロックし、ロックを解除するときは、予め設定されたパスワードをダイヤルキーから入力するものが存在する。しかし、このような移動通信端末装置ではキー入力をロックするために利用者自らが所定の操作を行う必要がある。このため、利用者が必要な操作をするのを忘れていたり、煩雑さを嫌ってロックを怠ってしまうといったケースが起きやすく、個人情報の保護機能としては十分に機能しているとは言い難いのが実状である。

【０００４】また、移動通信端末装置にＳＩＭ（Subscriber Identity Module）カードを実装する場合、端末交換時の作業を容易にするために、開閉が比較的容易な部位にインタフェースを設けることが多いが、このことは第三者が不正に移動通信端末装置からＳＩＭカードを取り外す場合であっても作業が容易であることを意味する。

【０００５】更に、移動通信端末装置の筐体はネジ等の接合部材を用いて組み立てられていることが多いが、従来の筐体ではネジ穴が露出しているか、簡単に取り外し可能なゴムのキャップが被せてあるだけの場合がある。

このような移動通信端末装置は簡単に分解されてしまうので、やはりデータ保護の観点から見ると問題がある。

【０００６】

【発明が解決しようとする課題】このような状況に鑑みて、本発明が解決しようとする課題は、正規の利用者以外の者による利用を制限することができる折り畳み型移動通信端末装置を提供することである。

【０００７】

【課題を解決するための手段】上記の課題を解決するため、本発明は次のような移動通信端末装置を提供する。即ち、本発明は、第１及び第２の筐体を開閉手段で接続した折り畳み型の移動通信端末装置において、開閉手段が閉じた状態をロックするロック手段と、ロック手段が開閉手段をロックしていることを検知する開閉検出手段と、予め登録された利用者を認証する認証手段と、認証手段による認証結果に応じて、ロック手段によるロックを解除する制御手段とを備えることを特徴とする移動通信端末装置を提供する。このような移動通信端末装置によれば、認証手段により利用者と認証されない限り、第１及び第２の筐体部を折り畳んだ状態から開いた状態にすることができないので、利用者以外の者が不正に移動通信端末装置を利用しないようにすることができる。

【０００８】この移動通信端末装置において、第１及び第２の筐体のそれぞれが、接合部材により互いに嵌合する少なくとも２つの部材からなり、接合部材の少なくとも一部は、開閉手段が閉じた状態にあるとき第１及び第２の筐体により隠蔽され、開閉手段が開いた状態にあるとき露呈することとしてよい。こうすれば、第１及び第２の筐体を分解することが困難になるので、移動通信端末装置内に格納された情報の安全性を高めることができる。尚、代表的な接合部材としてはネジがある。このとき隠蔽されるのはネジの頭部である。

【０００９】この移動通信端末装置は、取り外し可能な装置と接続するためのインタフェースを備え、開閉手段が閉じた状態でインタフェースを隠蔽することとしてもよい。この場合、利用者に無断でインタフェースに外部装置を接続されたり、既に接続してある装置を無断で取り外されてしまうのを防ぐことができる。ここでいう取り外し可能な装置としては、例えば記憶装置がある。

【００１０】この移動通信端末装置において、制御手段は、開閉検出手段によって、開閉手段が閉じた状態にあることを検出した時間が予め定められた時間を経過すると、ロック手段によって、開閉手段をロックすることとしてよい。この場合、利用者が意識的にロックしなくても一定時間が経過すると自動的にロックされる。

【００１１】この移動通信端末装置において、ロック手段が開閉手段をロックすると、受け付ける操作を制限し、認証手段が利用者を認証すると、制限を解除することとしてよい。この場合、ロックされた筐体を無理やりこじ開けたとしても、利用可能な機能が制限される。

【００１２】この移動通信端末装置において、認証手段の例としては、指紋に基づいて認証を行うもの、音声入力手段を含み、音声に基づいて認証を行うもの、押下するキーの組み合わせに基づいて認証を行うもの、画像入力手段を含み、入力された画像に基づいて認証を行うもの、無線受信手段を含み、外部装置から無線を介して入力された情報に基づいて認証を行うもの等が考えられる。

【００１３】

【発明の実施の形態】１．移動通信端末装置１００の基本構成

本発明の一実施の形態である移動通信端末装置１００について説明する。図１を参照すると、移動通信端末装置１００は、制御部１、メモリ２、ロック機構３、認証部４、表示部５、操作部６及び開閉検出部７からなる。制御部１は、電話端末としての発着信動作、メーラー、アドレス帳等の各種動作の実行及び制限、表示部５の点灯制御を行う。メモリ２は、正規の利用者のパターンデータを登録パターンとして予め格納しておく。例えば、認証部４が指紋による認証を行う場合、メモリ２は正規利用者の指紋パターンを格納することになる。ロック機構３は、移動通信端末装置１００の折り畳み状態を維持するための機構であり、制御部１からの指示に応じて開閉機構を物理的にロックする。認証部４は、認証の際に照会するパターンデータ（照会パターン）を入力する手段を備え、照会パターンとメモリ２に格納されている登録パターンとのマッチングを行う。認証部４の入力手段は折り畳み状態であっても入力可能であるように配置される。例えば、指紋による認証を行なうのであれば、指紋の読み取り面は移動通信端末装置を折り畳んだ状態で外部に露出するように配置される。しかし、電磁波を介して認証を行なうのであれば入力手段は必ずしも外部に露出して配置しなくてもよい。表示部５は液晶等の画像出力装置である。操作部６はダイヤルキー、各種ファンクションキー等の入力装置である。開閉検出部７は移動通信端末装置１００の開閉機構が開いているのか閉じているのかを検出する。

【００１４】２．移動通信端末装置１００の動作

次に、移動通信端末装置１００の動作について説明する。正規利用者の認証に必要となる登録パターンはメモリ２に予め格納しておくものとする。

【００１５】（１）折り畳んだときの動作

図２を参照すると、移動通信端末装置１００を折り畳むと、制御部１は次のような処理を行なう。即ち、開閉検出部７が移動通信端末装置１００を折り畳んだことを検出すると、表示部５の表示を消灯（ステップＳ１）する。予め設定された時間が経過しても折り畳んだままの状態が維持されている（ステップＳ２）と、開閉機構のロック／解除を示すフラグであるLockFlgを１（ロック状態）に変更する（ステップＳ３）と同時に、ロック機

構３を作動させて、ロック状態に移行させる（ステップＳ４）。尚、LockFlgが１のとき制御部１は特定の操作のみを受け付けるものとする。ここで制御部１が受け付ける操作としては、認証部４による認証動作を開始するための操作や、１１０番や１１９番等に代表される緊急通信を行なうための操作である。

【００１６】（２）ロックを解除する動作

図３を参照すると、折り畳み後、設定された時間が経過した後に移動通信端末装置１００を利用する場合、まず、必要であれば認証部４による認証動作を開始するための操作を行なう。次に、照会パターンの入力を認証部４にて受け付け（ステップＳ５）、メモリ２に格納されている登録パターンを読み出し（ステップＳ６）て、両者を比較する（ステップＳ７）。両者が一致する場合、LockFlgを０に変更する（ステップＳ８）と共に、ロック機構３を作動させてロックを解除させる（ステップＳ９）。尚、ステップＳ５～Ｓ９の処理を経た後、更に設定時間を経過しても移動通信端末装置１００を開かなかった場合、制御部１はロック機構３を再度作動させて、ロック状態に戻す。

【００１７】（３）開くときの動作

図４を参照して説明すると、移動通信端末装置１００を開くと、制御部１は次のように動作する。まず、制御部１はLockFlgが０であるかどうか確認する（ステップＳ１０）。ここでLockFlgが０である場合、ステップＳ７で正規利用者として認証されていることになるので、表示部５を表示させて通常通りに利用者からの操作を受け付けるようにする（ステップＳ１１）。他方、ここでLockFlgが１である場合、ステップＳ７で正規利用者として認証されていないことを意味する。このときはそのまま処理を終了し、特定の操作（認証動作の開始や緊急通信を行なう操作）以外の操作は全て無効とする。

【００１８】（４）発信操作の受付

図５を参照して移動通信端末１００による発信操作の受付動作について説明する。ダイヤルキーへの入力があると、制御部１はLockFlgの値を参照する（ステップＳ１２）。LockFlgが０である場合、正規利用者によりロックが解除されているので緊急通信であるか否かに関わらず発信を行なう。他方、LockFlgが１である場合、緊急通信であるかどうかを判定する（ステップＳ１３）。例えば、発信相手番号が予め緊急通信先の番号として登録されている番号である場合、その発信は緊急通信であると判定し、その番号に発信する。緊急通信先として登録されていない番号の場合、その発信は無効となる。

【００１９】３．ロック機構３の例

次にロック機構３の例を図面を参照して説明する。

【００２０】（１）ロック機構３の例１

図６を参照して説明する。移動通信端末装置１００は筐体８と筐体９が開閉機構１０により接続された構造を有する。筐体８及び９はそれぞれスリット１１及び１２を備える。スリット１１及び１２は開閉機構１０を閉じたとき互いに一致するように配置されている。筐体８は更に回転子１３をスリット１１の内部に備える。回転子１３は制御部１の指示に応じて回転する。ロックを解除した状態では、回転子１３は図６右側上段のようになっている。ステップＳ４において、回転子１３は半時計方向に回転し、開閉機構１０が開かないようにロックする。また、この状態から、ステップＳ９において、回転子１３は時計方向に回転し、ロックを解除した状態となる。

【００２１】（２）ロック機構３の例２

次に図７を参照してロック機構３の他の例について説明する。この例では、筐体８はスリット１４を備える。スリット１４は開閉機構１０の回転に応じて筐体９に対する位置を変える。一方、筐体９は開閉機構１０に接する端部にスライドバー１５を備える。スライドバー１０は制御部１の指示に応じて動作し、筐体９の内部に収納される状態と、筐体９から突出した状態とをとる。ステップＳ４において、スライドバー１５は筐体９の外部に突出するように動作してスリット１４に嵌合し、開閉機構１０が開かないようにロックする。また、この状態から、ステップＳ９において、スライドバー１５は筐体９の内部に引っ込むことにより、ロックを解除した状態となる。

【００２２】４．認証部４の例

（１）指紋による認証１

認証部４の例について図８を参照して説明する。この例では、指紋を用いて利用者を認証する。移動通信端末装置１００の筐体外面で折り畳んだ状態でも操作可能な部位に、認証開始キー２１及び指紋読取部２２を備える。認証開始キー２１は利用者が指で押下あるいはスライドさせることによりオンになるスイッチであり、このスイッチをオンにすると指紋読取部２２が指紋の読取動作を開始する。この例の場合、メモリ２に格納される登録パターンは指紋の読取パターンとなり、ステップ５では、利用者が認証開始キー２１をオンにして、指紋読取部２２は読取動作を開始し、照会パターンを取得する。

【００２３】（２）指紋による認証２

認証部４の他の例について図９を参照して説明する。この例でも指紋を照会パターンとして取得し、メモリ２に予め格納した登録パターンと比較して認証を行なうが、認証開始キーと指紋読取部の配置が異なる。認証開始キー２３は筐体側面に配置される。また、指紋読取部２４は、図９のように、使用しないときは筐体内部に収納され、使用するときに引き出されるようになっている。

【００２４】（３）入力したキーの順列による認証

この例の場合、移動通信端末装置１００は折り畳んだ状態で操作可能な部位に複数のキーを備え、これらのキーを操作する順列に応じて認証を行なう。例えば、図１０のように、筐体側面にキー２５、２６及び２７を設けてそれぞれ順にキーA、B、Cとすると共に、B、A、

Ａ、Ｃ、Ａの順列を予めメモリ２に登録パターンとして格納しておく。ステップＳ５において、利用者が登録パターンと一致する順番にキー操作を行なった場合、即ち、この例ではキーＢ、Ｂ、Ａ、Ａ、Ｃ、Ａの順番に操作した場合、ステップＳ７において正規利用者として認証する。

【００２５】（４）音声認識による認証

この場合、認証部４は、音声を入力するマイクと、入力された音声から話者の音声パターンを抽出する音声パターン抽出手段を備える。図１１のように、移動通信端末装置１００には、認証開始キー２８及びマイク２９が折り畳んだ状態で外側になるように配置される。ステップ５でパターン検出を行なうには、まず利用者が認証開始キー２８を押し、続いてマイク２９に対して話し掛けると、音声パターン抽出手段が音声パターンを抽出する。ステップ６でメモリ２に予め格納されている正規利用者の音声パターンを取得し、ステップ７でこれらの音声パターンを比較して正規利用者か否かを判定する。

【００２６】（５）画像認識による認証

この場合、認証部４は、画像を入力するカメラと、入力された画像からパターンを抽出する画像パターン抽出部とを備える。図１２のように、移動通信端末装置１００には、認証開始キー３０及びカメラ３１が折り畳んだ状態で外側になるように配置される。ステップ５でパターン検出を行なうには、まず利用者が認証開始キー３０を押し、続いてカメラ３１に例えば顔を撮影させると、画像パターン抽出手段が顔の画像パターンを抽出する。ステップ６でメモリ２に予め格納されている正規利用者の顔の画像パターンを取得し、ステップ７でこれらの画像パターンを比較して正規利用者か否かを判定する。

【００２７】（６）無線を利用した認証

この例では、認証部４は、例えばブルートゥースのような短距離無線手段を備える。また、この短距離無線手段に対応する無線装置を移動通信端末装置１００の他に用意し、この無線装置を予め移動通信端末装置１００に登録しておく。メモリ２には無線装置の登録データがパターンとして格納される。登録された無線装置は移動通信端末装置１００を利用する際の鍵の役割をする。認証を行なう際には、移動通信端末装置１００に設けた認証開始キーを押した後で無線装置から発信してもよい。あるいは、登録された無線装置から受信しているときはロック解除状態とし、受信していないときはロック状態としてもよい。

【００２８】５．不正な分解からの保護

移動通信端末装置１００では、筐体が分解されたり、内蔵された記憶装置が不正に取り外されてしまうのを防ぐことができる。

【００２９】（１）筐体の分解防止

図１３に図示した例では、筐体８及び９は共に開閉機構１０の側に設けられた２本の組立ネジ３２を締結することにより組み立てられている。これらの組立ネジ３２の頭部はいずれも移動通信端末装置１００を折り畳んだ状態にすると対向する筐体により隠蔽されるように配置される。従って、組立ネジ３２を緩めて筐体８及び９を分解するためには、まず移動通信端末装置１００を開いた状態にしなければならない。これにより、移動通信端末装置１００を第三者が不正に分解することを防ぐことができる。

【００３０】（２）SIMカードの保護

図１４に図示した例では、筐体９の主入力キー部３３は開閉可能になっており、その下にはＳＩＭカード３４が配置されている。このような構造を有することにより、SIMカード３４を取り外す場合、先に移動通信端末装置１００を開かなければならなくなる。よって、第三者が不正にSIMカード３４を取り外すのを防ぐことができる。

【００３１】以上、本発明を実施の形態に基づいて説明したが、本発明はこれに限定されるものではなく、当業者の通常の知識の範囲内でその変更や改良が可能であることは勿論である。

【００３２】

【発明の効果】本発明の移動通信端末装置によれば、認証手段により利用者と認証されない限り、折り畳んだ状態から開いた状態にすることができないので、利用者以外の者が不正に移動通信端末装置を利用しないようにすることができる。

【００３３】また、本発明によれば、移動通信端末装置内に格納された情報の安全性を高めることができる。

【００３４】また、本発明によれば、利用者に無断でインタフェースに外部装置を接続されたり、既に接続してある装置を無断で取り外されてしまうのを防ぐことができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態である移動通信端末装置１００の機能ブロック図である。

【図２】移動通信端末装置１００の動作を説明するフローチャートである。

【図３】移動通信端末装置１００の動作を説明するフローチャートである。

【図４】移動通信端末装置１００の動作を説明するフローチャートである。

【図５】移動通信端末装置１００の動作を説明するフローチャートである。

【図６】ロック機構３の一例を説明する図である。

【図７】ロック機構３の一例を説明する図である。

【図８】認証部４の一例を説明する図である。

【図９】認証部４の一例を説明する図である。

【図１０】認証部４の一例を説明する図である。

【図１１】認証部４の一例を説明する図である。

【図１２】認証部４の一例を説明する図である。

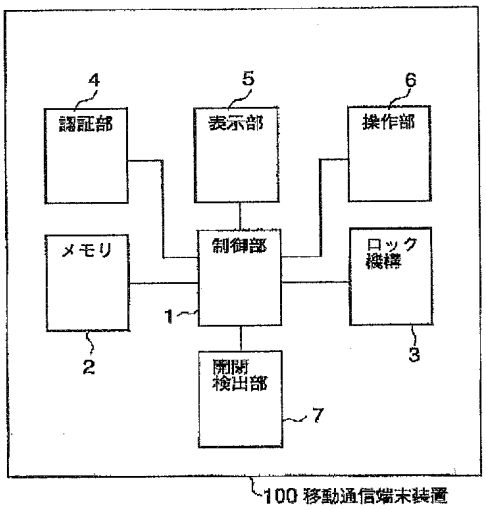
【図１３】移動通信端末装置１００を組み立てるネジ３２の配置を説明する図である。

【図１４】SIMカードの配置を説明する図である。

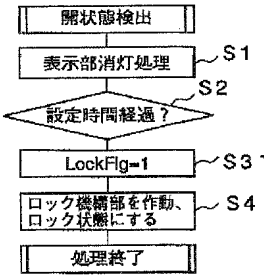
【符号の説明】

１　制御部
２　メモリ
３　ロック機構
４　認証部
５　表示部
６　操作部
７　開閉検出部
１０　開閉機構
１１、１２、１４　スリット
１３　回転子
１５　スライドバー
２１、２３、２８、３０　認証開始キー
２２、２４　指紋読取部
２５、２６、２７　キー
２９　マイク
３１　カメラ
３２　組立ネジ
３３　主入力キー部
３４　ＳＩＭカード

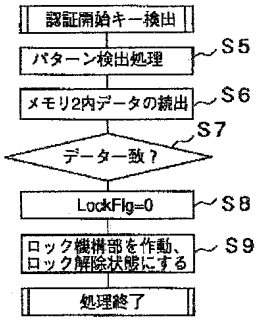
【図１】



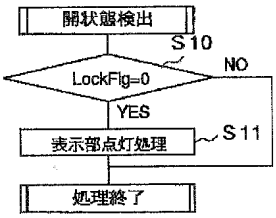
【図２】



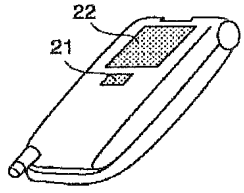
【図３】



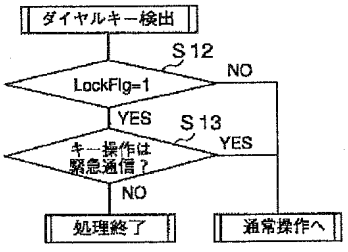
【図４】



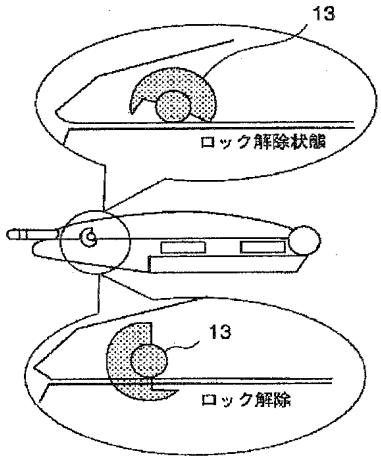
【図８】



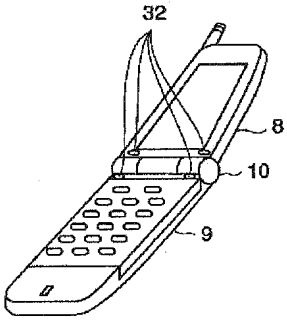
【図５】



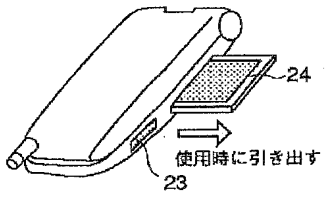
【図６】

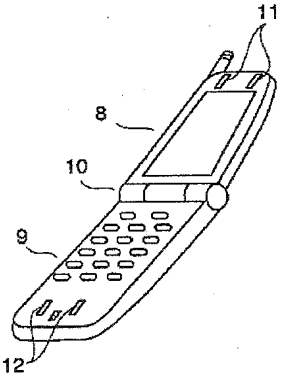


【図１３】

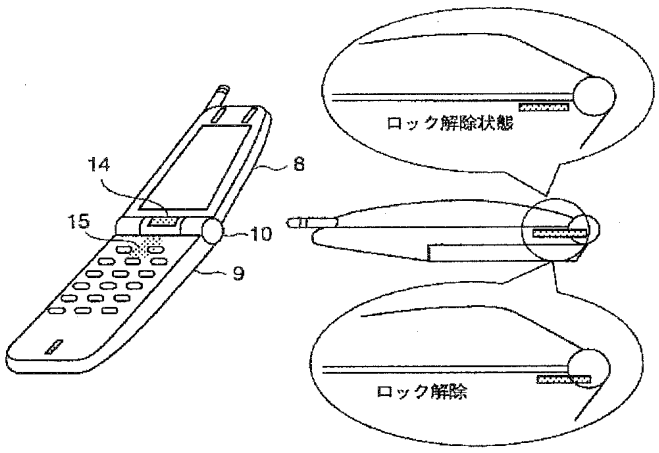


【図９】

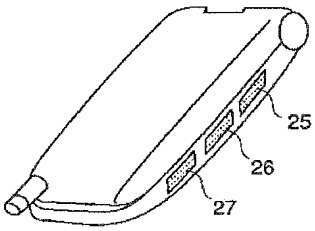




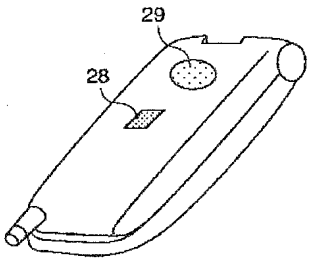
【図７】



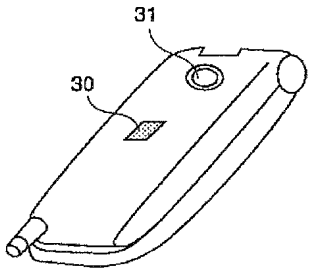
【図１０】



【図１１】



【図１２】



【図１４】